“Privacy is a **fundamental human right** … Privacy underpins human dignity and other key values such as freedom of association and freedom of speech.”

Source: *Privacy International, Sept 2015*

REALITY is a little messy

- Privacy means different things in different countries.
- Privacy means different things to different generations.
- Privacy requires implementation of security control… controls which may subvert the goals of privacy protection.

Percentage of millenials who would be willing to give away more personal information for a better on-line shopping experience?

1. 56%
2. 23%
3. 7%

Percentage of millenials who would be willing to give away more personal information for a better on-line shopping experience?

1. [✓ 56%]
2. 23%
3. 7%

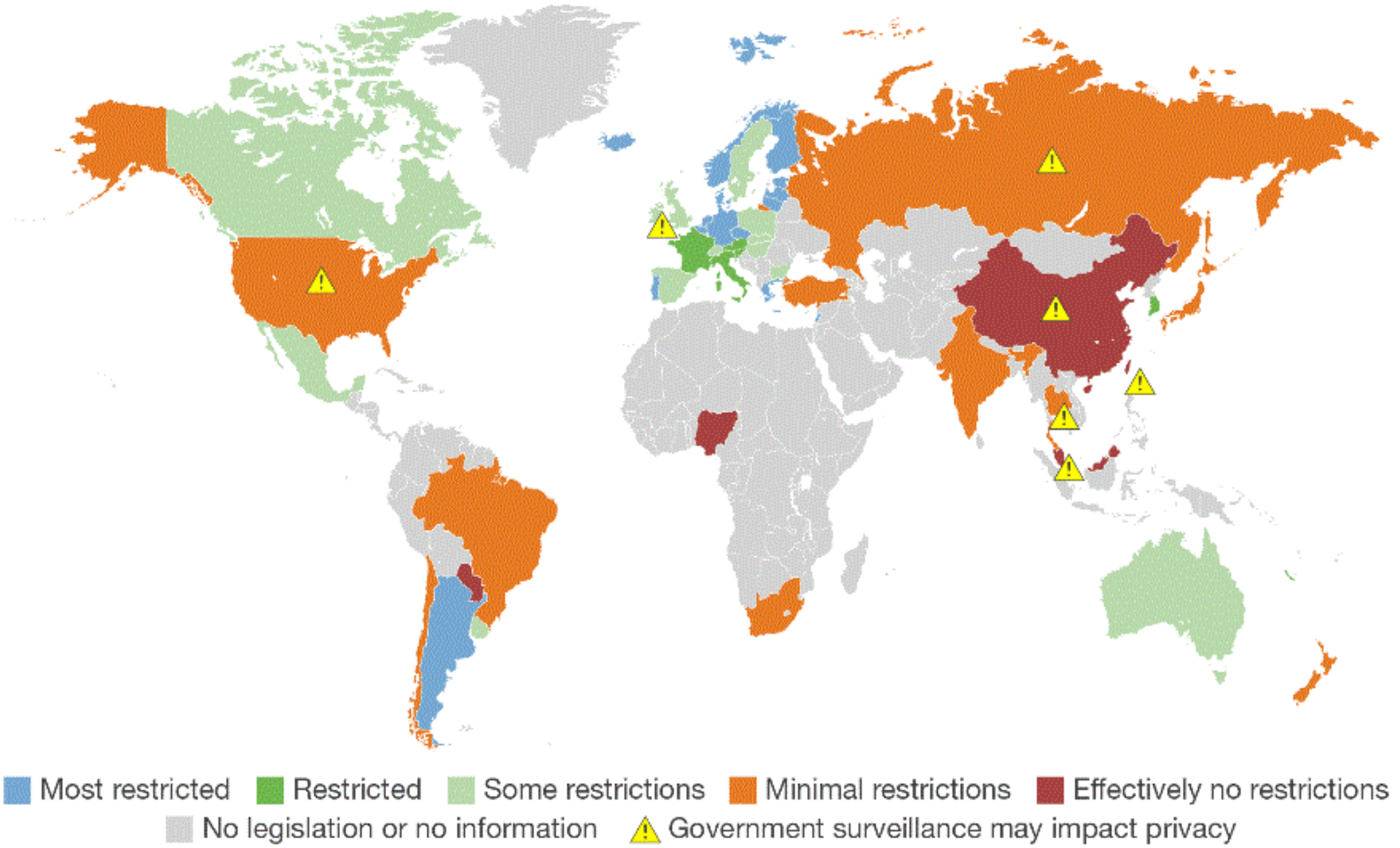
Source: Direct Marketing Association

Top 3 Drivers of Privacy Protection (aka Privacy) Regulation World-Wide

- **To promote electronic commerce.** Many countries, especially in Asia, Canada and the U.S., have developed laws in an effort to promote electronic commerce. These countries recognize consumers are uneasy with their personal information being sent worldwide.
- **To ensure laws are consistent with Pan-European laws.** Most countries in Central and Eastern Europe are adopting new laws based on the Council of Europe Convention and the European Union Data Protection Directive.
- **To remedy past injustices.** Many countries, especially in Central Europe, South America and Africa, are adopting laws to remedy privacy violations that occurred under previous authoritarian regimes.

Source: Privacy and Human Rights - http://gilc.org/privacy/survey/intro.html

The patchwork of privacy laws


Most restricted
Restricted
Some restrictions
Minimal restrictions
Effectively no restrictions
No legislation or no information
⚠ Government surveillance may impact privacy

SOURCE: Forrester’s 2014 Data Privacy Heat Map

Practically (my definition)…

PRIVACY: The right of an **individual** to

- Control your own personal information,
- Not have it disclosed, used or modified by others without permission.

Privacy protection regulations require:

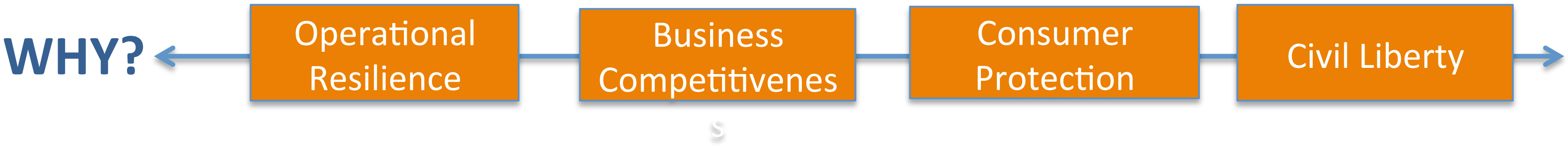
- Be accountable — Establish ownership and accountability within the organization for confidentiality, integrity, and availability
- Identify & document purposes — Identify the reasons for obtaining private information from an end user, make those reasons available to the end user
- Ensure consent — Establish mechanisms for gaining consent of the end user before collecting private information
- Limit collection — Limit collection of private information to only that information you need for business purposes
- Limit use, disclosure and retention — Limit use, disclosure only for the purposes for which you have gained consent. Limit retention of information to a time period specified by law and/or consent
- Ensure accuracy — Ensure that information collected is accurate
- **Implement safeguards — Implement administrative, technical, and physical controls around information in order to ensure its confidentiality, integrity, and availability**
- Create openness — Create a culture of openness, so that if the confidentiality, integrity or availability of the information is breached in a significant way that the end user is notified
- Provide recourse — Provide the end user with documented escalation policy and process.

SECURITY is the means used to protect the confidentiality, availability and integrity of personal information through physical, technical and administrative safeguards.

WE LOST ALL OF OUR COMPANY DATA AND OUR BACKUPS, TOO.
Dilbert.com DilbertCartoonist@gmail.com
SO I HACKED INTO OUR GOVERNMENT'S SECRET DATABASE WHERE THEY KEEP RECORDS OF EVERY-THING WE SAY OR DO AND GOT IT ALL BACK.
9-6-13 ©2013 Scott Adams, Inc.
I FEEL AS IF I SHOULD BE DOING SOMETHING NOW.
NAH. EVERY-THING IS WORKING FINE.

COMMERCIAL BREAK: Privacy Protection is only one of 4 risk domains involving/leveraging Security

The BIG Four	Cyber War/Unrest (Emerging Focus)	Cyber Espionage (Emerging Focus)	Cyber Crime (Existing Focus)	Privacy
Basic Requirement:	▪ Assure the availability and integrity of critical infrastructure assets for the purpose of ensuring the public good	▪ Assure the confidentiality, integrity, and availability of select data sets considered “crown jewel” by the organization.	▪ In order to mitigate the risk of money laundering, fraud the general requirement is to protect integrity, availability and authenticity of financial transactions	▪ Assure the confidentiality, integrity, and availability of personally identifiable information in order to protect fundamental human rights
Buzzwords:	▪ Cyber Warfare ▪ Hacktivism	▪ Cyber Espionage	▪ Money Laundering ▪ Fraud ▪ *Identity Theft*	▪ Privacy ▪ *Identity Theft*
Concern owner:	▪ IT Security	▪ CISO ▪ Legal Officer	▪ Financial Crime Unit	▪ Chief Privacy Officer



WHY?

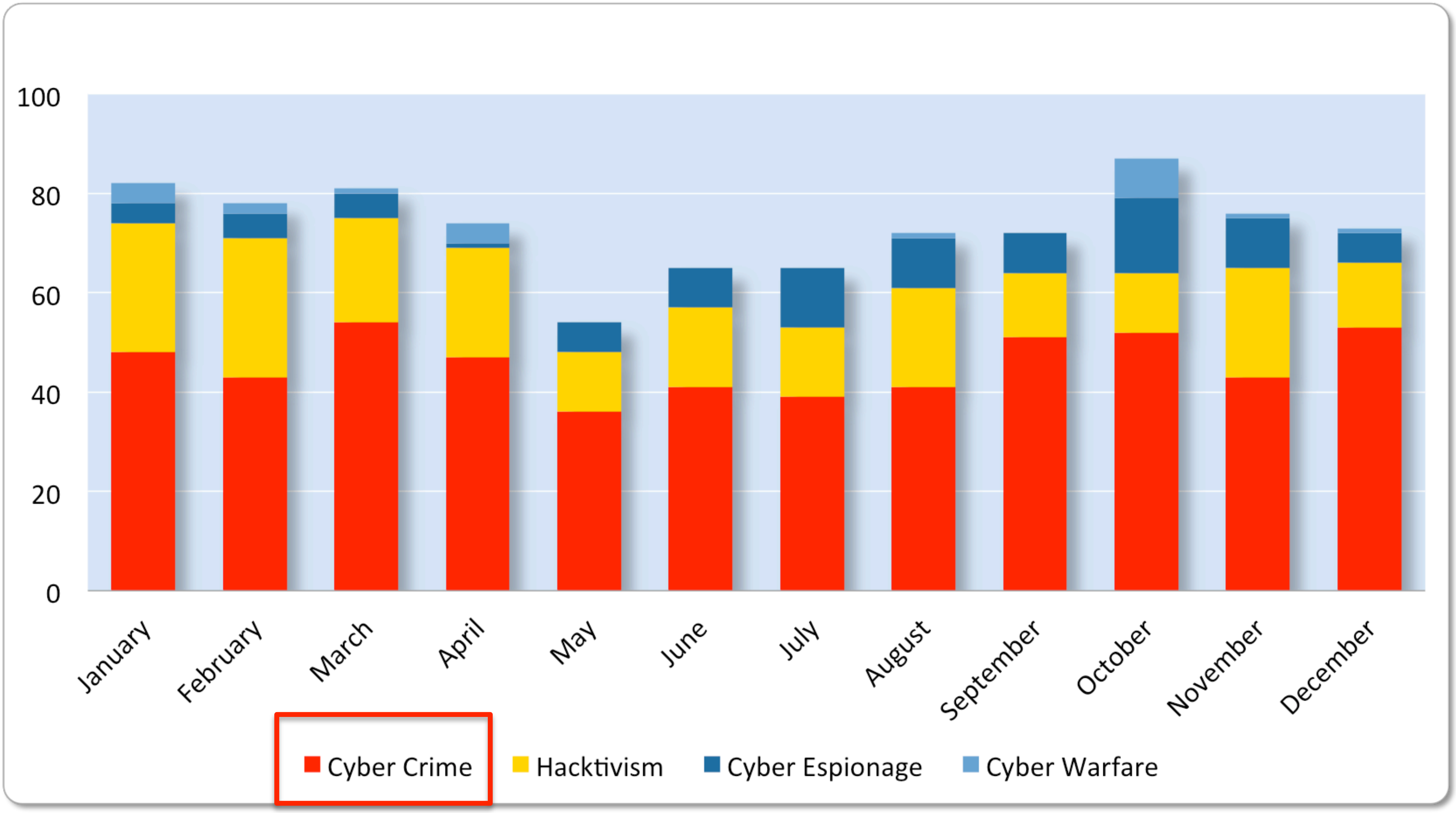
Operational Resilience

Business Competitiveness

Consumer Protection

Civil Liberty

Practically, what do businesses worry about (risk)?



Source: Hackmaggedon Index 2014

Security reality – we have all been compromised

1,764,121

Represents the number of security events the average organization of 15K employees will capture weekly

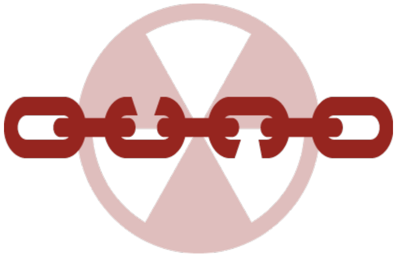
324 of these events represent actual attacks, per week

2.1 of these attacks will result in an **incident**, **per week, –** a 22% annual increase

2014 IBM Cybersecurity Intelligence Index

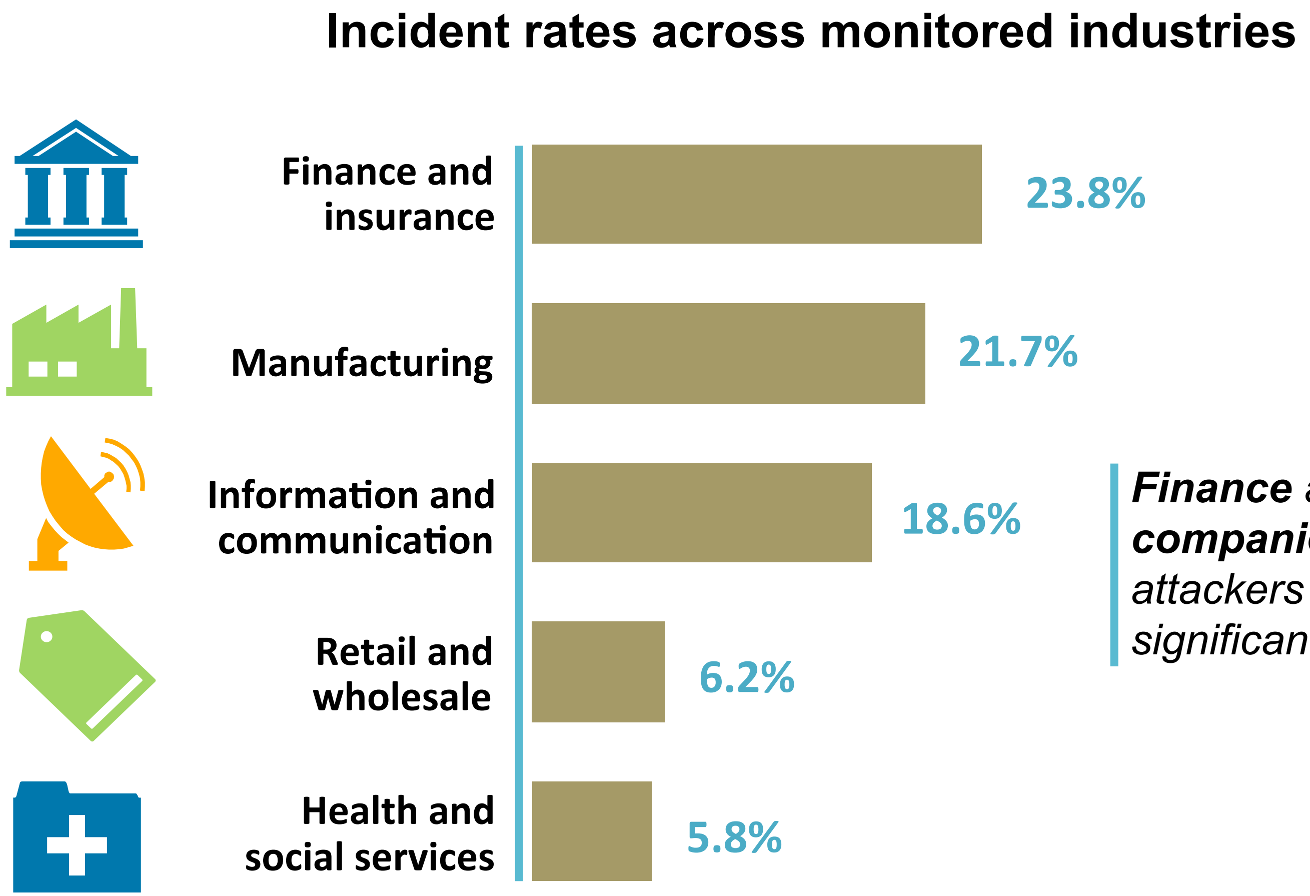
only 1 out of 100

security compromises **are ever detected**



General Keith Alexander, Head of U.S. Cyber Command, in a speech to the American Enterprise Institute

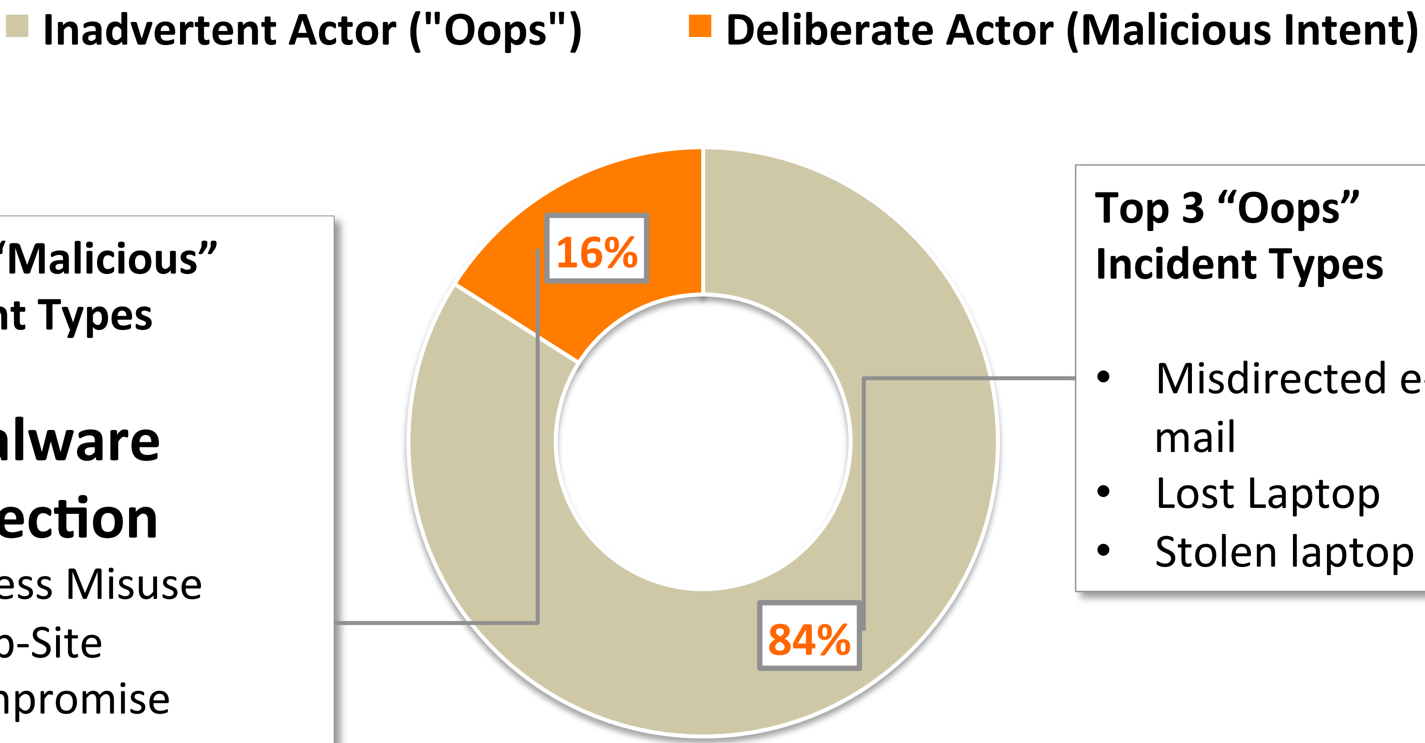
Over 75% of incidents were associated with the same five industries



***Finance** and **insurance companies** tend to offer attackers the most significant potential payoff*

Source: IBM Security Services 2014 CyberSecurity Intelligence Index

From a practitioner's perspective, most security incidents are of the "Oops" variety



Top 3 "Malicious" Incident Types

- **Malware Infection**
- Access Misuse
- Web-Site Compromise

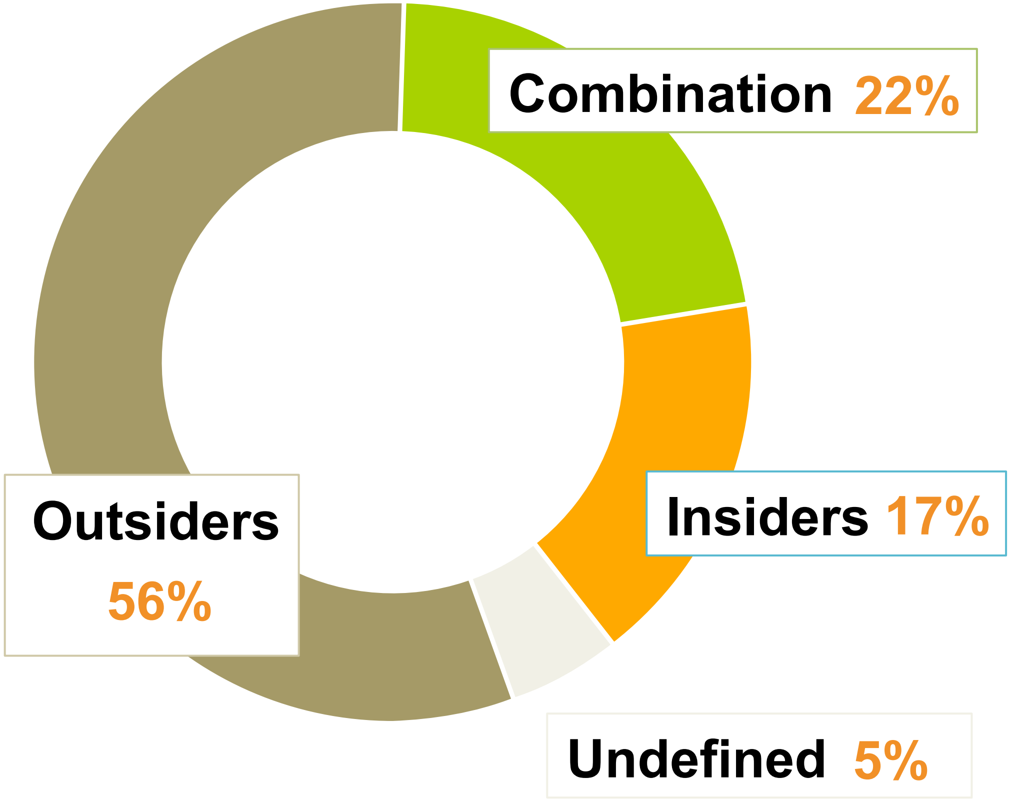
~1% of all malicious attack result are "noteworthy"(possibly material/significant)

Top 3 "Oops" Incident Types

- Misdirected e-mail
- Lost Laptop
- Stolen laptop

While threat actors are acting “maliciously”, insiders are an “unwitting” accomplice in 95% of incidents

Who’s attacking



Who’s letting them in

“...over 95% of all incidents investigated recognize “human error” as a contributing factor.”

Source: IBM Security Services 2014 CyberSecurity Intelligence Index

Top 5 reasons WHY compromise was possible

End users

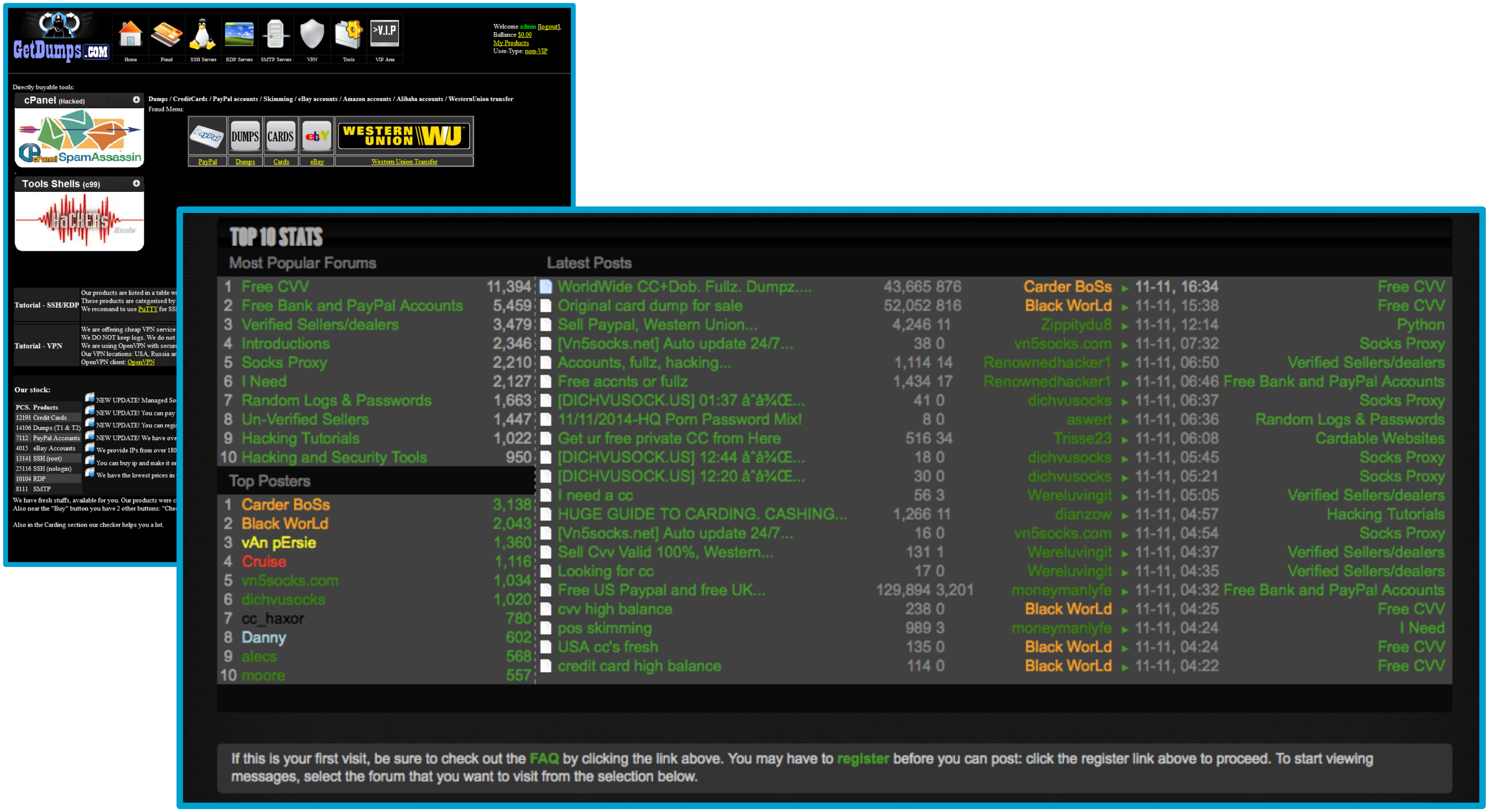
1. Double-clicking "on anything", plugging "anything" (like a USB) in
2. Disabling security settings and/or anti-virus when it gets in the way
3. Using vulnerable, legacy software and hardware
4. Failing to install security patches ("Remind me Tomorrow")
5. Using a weak or default passwords, or using business passwords for personal use

Systems Admins/Developers

1. Connecting systems and virtual images to the Internet before hardening them
2. Failing to remove default accounts or passwords, failing to remove old/ unused user accounts
3. Failing to update or patch systems/ applications on a timely basis.
4. Using legacy or end-of-life software and hardware
5. Using insecure remote management software

Why is it crime so easy? IT'S BIG BUSINESS.

Data is bought an sold in "carding forums"



Welcome admin [logout],
Ballance $0.00
My Products
User-Type: non-VIP

Directly buyable tools:

Dumps / CreditCards / PayPal accounts / Skimming / eBay accounts / Amazon accounts / Alibaba accounts / WesternUnion transfer

Fraud Menu:

PayPal | Dumps | Cards | eBay | Western Union Transfer

Tutorial - SSH/RDP	Our products are listed in a table wi These products are categorised by We recomand to use PuTTY for SS
Tutorial - VPN	We are offering cheap VPN service We DO NOT keep logs. We do not We are using OpenVPN with secure Our VPN locations: USA, Russia an OpenVPN client: OpenVPN

Our stock:

PCS.	Products
12191	Credit Cards
14106	Dumps (T1 & T2)
7112	PayPal Accounts
4015	eBay Accounts
13141	SSH (root)
25116	SSH (nologin)
10104	RDP
8111	SMTP

- NEW UPDATE! Managed So
- NEW UPDATE! You can pay
- NEW UPDATE! You can regis
- NEW UPDATE! We have ove
- We provide IPs from over 180
- You can buy ip and make it or
- We have the lowest prices in

We have fresh stuffs, available for you. Our products were c
Also near the "Buy" button you have 2 other buttons: "Che

Also in the Carding section our checker helps you a lot.

TOP 10 STATS

Most Popular Forums		
1	Free CVV	11,394
2	Free Bank and PayPal Accounts	5,459
3	Verified Sellers/dealers	3,479
4	Introductions	2,346
5	Socks Proxy	2,210
6	I Need	2,127
7	Random Logs & Passwords	1,663
8	Un-Verified Sellers	1,447
9	Hacking Tutorials	1,022
10	Hacking and Security Tools	950

Top Posters		
1	Carder BoSs	3,138
2	Black WorLd	2,043
3	vAn pErsie	1,360
4	Cruise	1,116
5	vn5socks.com	1,034
6	dichvusocks	1,020
7	cc_haxor	780
8	Danny	602
9	alecs	568
10	moore	557

Latest Posts					
WorldWide CC+Dob. Fullz. Dumpz....	43,665	876	Carder BoSs	11-11, 16:34	Free CVV
Original card dump for sale	52,052	816	Black WorLd	11-11, 15:38	Free CVV
Sell Paypal, Western Union...	4,246	11	Zippitydu8	11-11, 12:14	Python
[Vn5socks.net] Auto update 24/7...	38	0	vn5socks.com	11-11, 07:32	Socks Proxy
Accounts, fullz, hacking...	1,114	14	Renownedhacker1	11-11, 06:50	Verified Sellers/dealers
Free accnts or fullz	1,434	17	Renownedhacker1	11-11, 06:46	Free Bank and PayPal Accounts
[DICHVUSOCK.US] 01:37 åˆå¾Œ...	41	0	dichvusocks	11-11, 06:37	Socks Proxy
11/11/2014-HQ Porn Password Mix!	8	0	aswert	11-11, 06:36	Random Logs & Passwords
Get ur free private CC from Here	516	34	Trisse23	11-11, 06:08	Cardable Websites
[DICHVUSOCK.US] 12:44 åˆå¾Œ...	18	0	dichvusocks	11-11, 05:45	Socks Proxy
[DICHVUSOCK.US] 12:20 åˆå¾Œ...	30	0	dichvusocks	11-11, 05:21	Socks Proxy
I need a cc	56	3	Wereluvingit	11-11, 05:05	Verified Sellers/dealers
HUGE GUIDE TO CARDING. CASHING...	1,266	11	dianzow	11-11, 04:57	Hacking Tutorials
[Vn5socks.net] Auto update 24/7...	16	0	vn5socks.com	11-11, 04:54	Socks Proxy
Sell Cvv Valid 100%, Western...	131	1	Wereluvingit	11-11, 04:37	Verified Sellers/dealers
Looking for cc	17	0	Wereluvingit	11-11, 04:35	Verified Sellers/dealers
Free US Paypal and free UK...	129,894	3,201	moneymanlyfe	11-11, 04:32	Free Bank and PayPal Accounts
cvv high balance	238	0	Black WorLd	11-11, 04:25	Free CVV
pos skimming	989	3	moneymanlyfe	11-11, 04:24	I Need
USA cc's fresh	135	0	Black WorLd	11-11, 04:24	Free CVV
credit card high balance	114	0	Black WorLd	11-11, 04:22	Free CVV

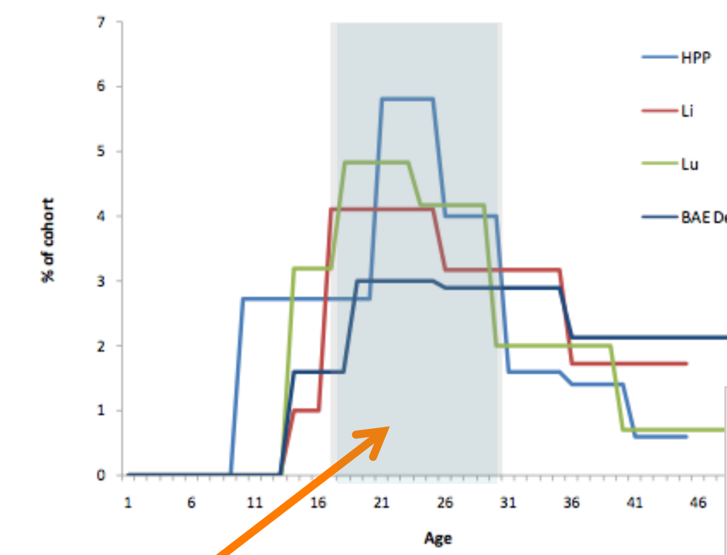
If this is your first visit, be sure to check out the FAQ by clicking the link above. You may have to register before you can post: click the register link above to proceed. To start viewing messages, select the forum that you want to visit from the selection below.

Attacks-as-service pricing models

Cost	Service Description
$350-$400 an hour	- Hacker consulting services
$100 per 1K installs	- Malware infection/spreading services
$535 for 5 hours a day for one week	- Distributed Denial of Service (DDoS) attack, money back guarantee
$40 / 20K emails	- Email spam
$2/30 posts	- Blog spam
$80 for 20K spammed backlinks	- Blackhat Search Engine Optimization (SEO)
$500 to $10K	- Crimeware, with premium support levels available
$150 and $400	- crack e-mail passwords in less than 48 hours

What keeps me up at night….

Figure 2.14: Age groups of cybercrime perpetrators



Source: UNODC elaboration of HPP, Li, Lu and BAE Detica

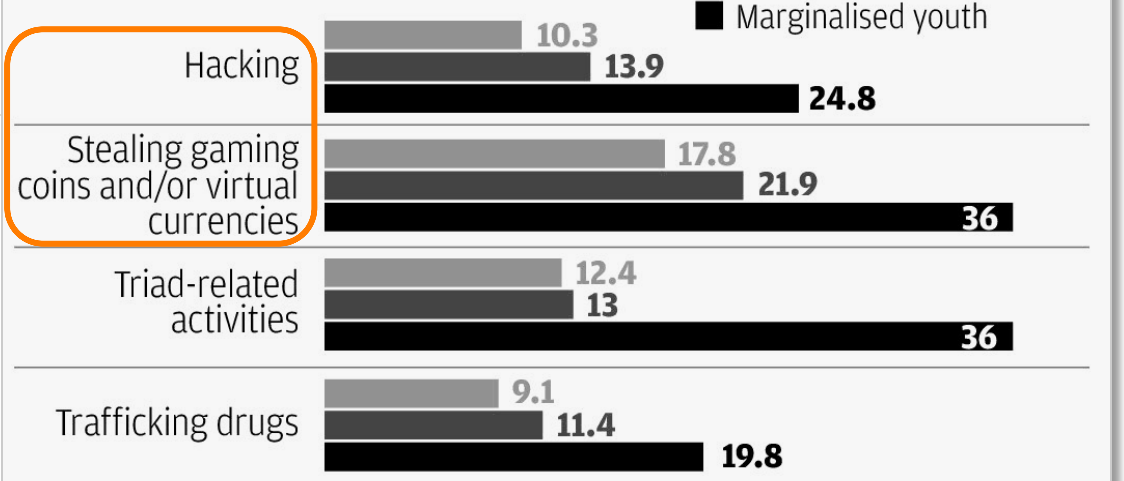
- By 2011, **~33%** of the world's population had access to the Internet.
- By 2017, that percentage will increase to **+70%**
- **45%** of all Internet users are currently **below the age of 25 years.**

"In the **developing country context** in particular, **sub-cultures of young men** engaged in computer-related financial fraud have emerged, **many of whom begin involvement in cybercrime in their late teenage years**…"

Source: UNODC 2013

Cyber juveniles

Those who have participated in... (%)

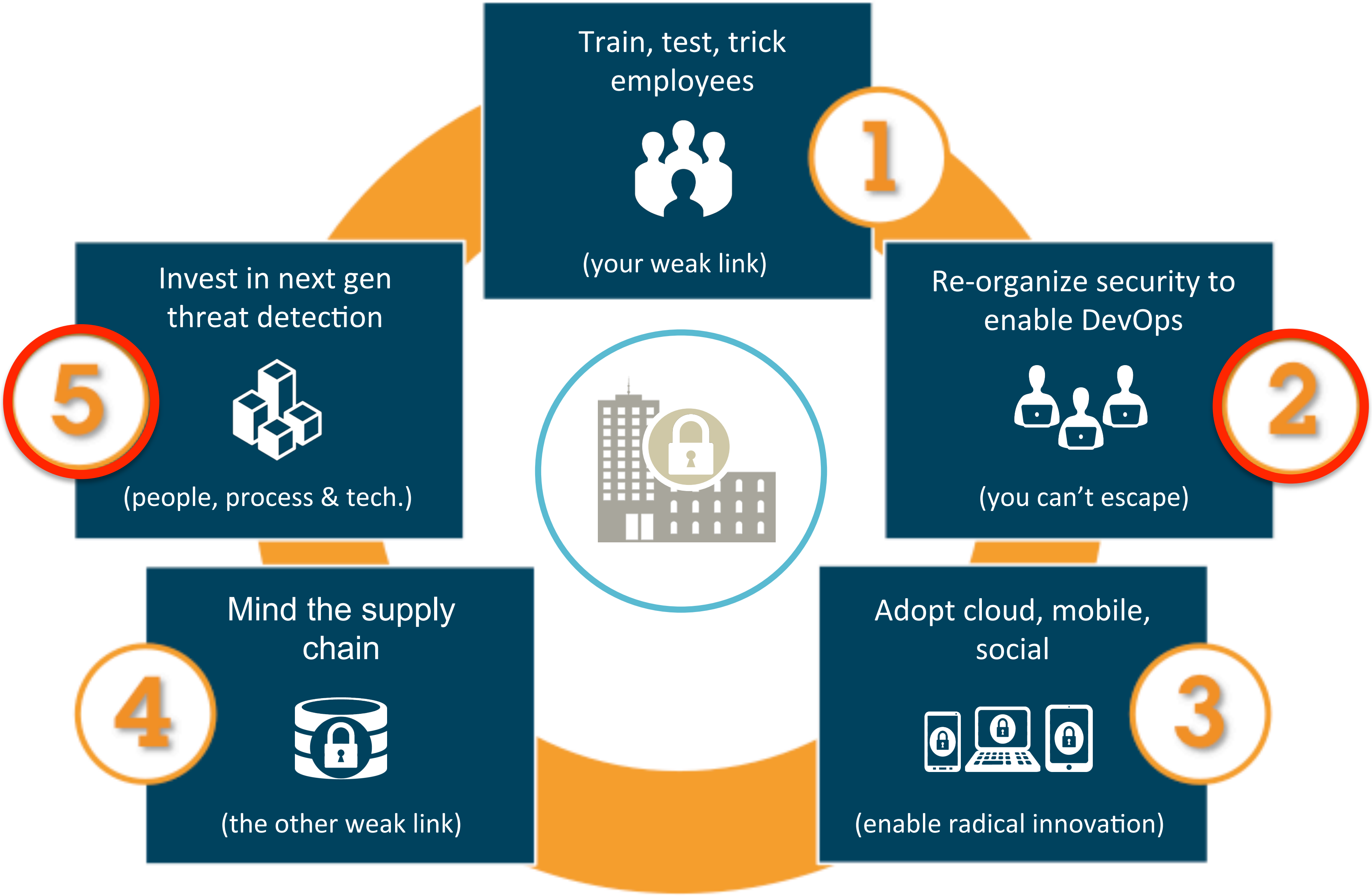


Source: Federation of Youth Group

SCMP

Recommendations

My big five focus areas



1 Train, test, trick employees

(your weak link)

2 Re-organize security to enable DevOps

(you can't escape)

3 Adopt cloud, mobile, social

(enable radical innovation)

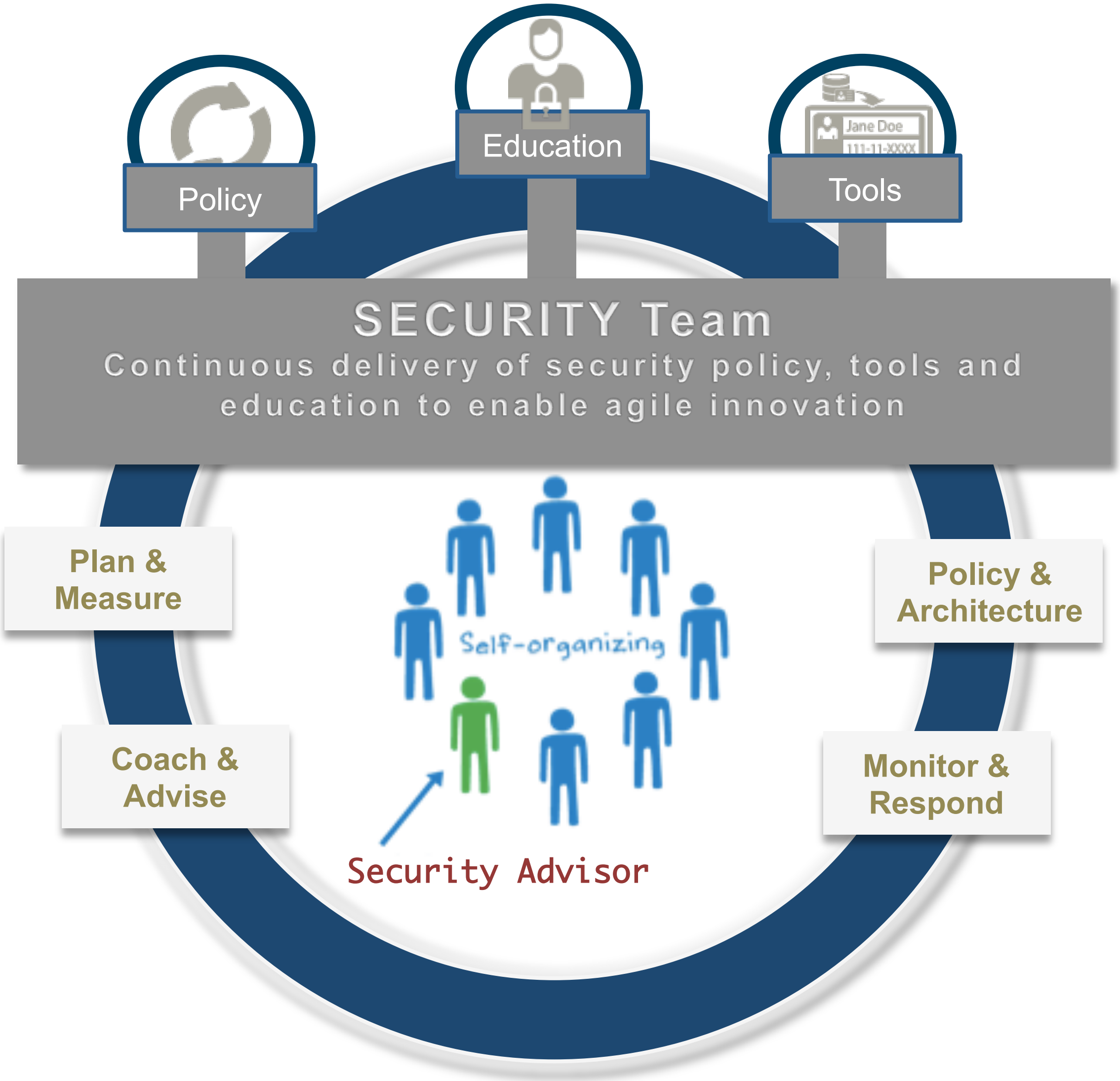
4 Mind the supply chain

(the other weak link)

5 Invest in next gen threat detection

(people, process & tech.)

Restructure to support the Agile/DevOps transformation



STRATEGIC PLANNING SERVICES

Define security strategy & objectives. Analyze metrics and measure effectiveness of controls. Drive continuous improvement.

POLICY & ARCHITECTURE SERVICES

Define the essential security policies , standards and architectures (based on 80/20 rule) which are easy to digest and consume.

COACHING & ADVISORY SERVICES

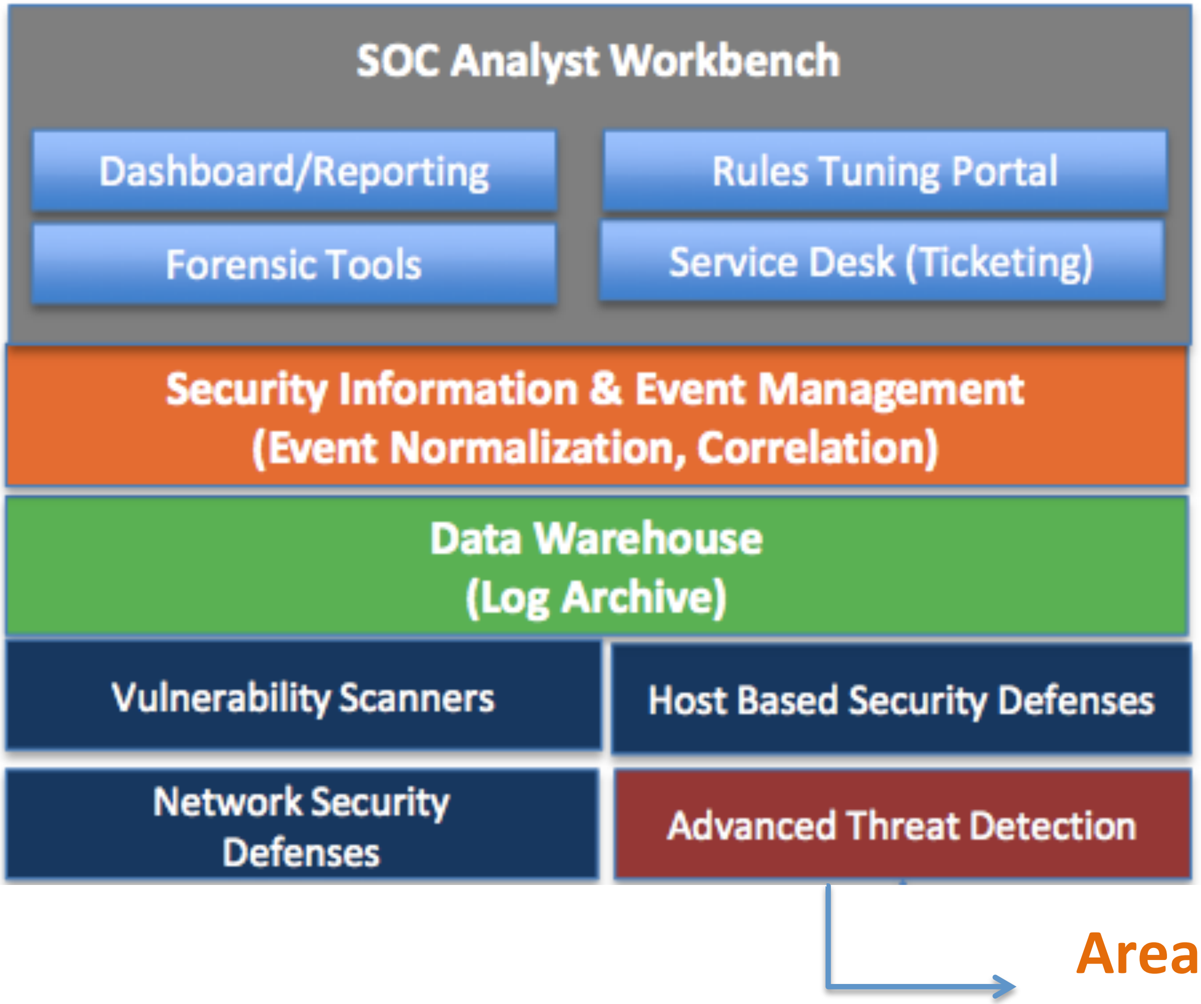
Staff domains with security subject matter expertise required to innovate with confidence. Increase security awareness through educational programs for employees and contractors.

SECURITY OPERATIONS

Provide core security monitoring, assessment & response services: Hunter Services, Threat Monitoring Services, and Incident Response

The emerging SOC (detection & response model)

Technology Platform



SOC Analyst Workbench

Dashboard/Reporting

Rules Tuning Portal

Forensic Tools

Service Desk (Ticketing)

Security Information & Event Management (Event Normalization, Correlation)

Data Warehouse (Log Archive)

Vulnerability Scanners

Host Based Security Defenses

Network Security Defenses

Advanced Threat Detection

Area of radical innovation!

Advanced threat detection via Machine Learning

- Machine learning is a process used to train computers to distinguish between classes of objects, and then to predict the class of an object they have never seen before using classifiers.

- Successfully applied in facial recognition, voice recognition, image processing, and medical diagnostics, it is being applied to cyber threat detection by enabling software classifiers to distinguish malware from benign software.

- Machine Learning has distinct advantages over traditional signature and sandbox-based approaches:

  - Scales to very high volumes of traffic,
  - Resilient to evolving malware and tactics,
  - Higher threat detection rates
  - Limited risk of privacy violation

Summary

- Privacy and security can co-exist, albeit uncomfortably.

- As broader cybersecurity regulation in EU and US is introduced, and impact of the Safe Harbor ruling is fully realized, the pendulum will swing from crisis driven security spending to compliance spending.

- Capabilities like Machine Learning will address trickier issues associated with security monitoring and analysis.

- Investments in DevOps (building security inside) is the only way to systemically “fix” our issues.

Thank you.

There are two reasons why organizations spend money on security

Crisis

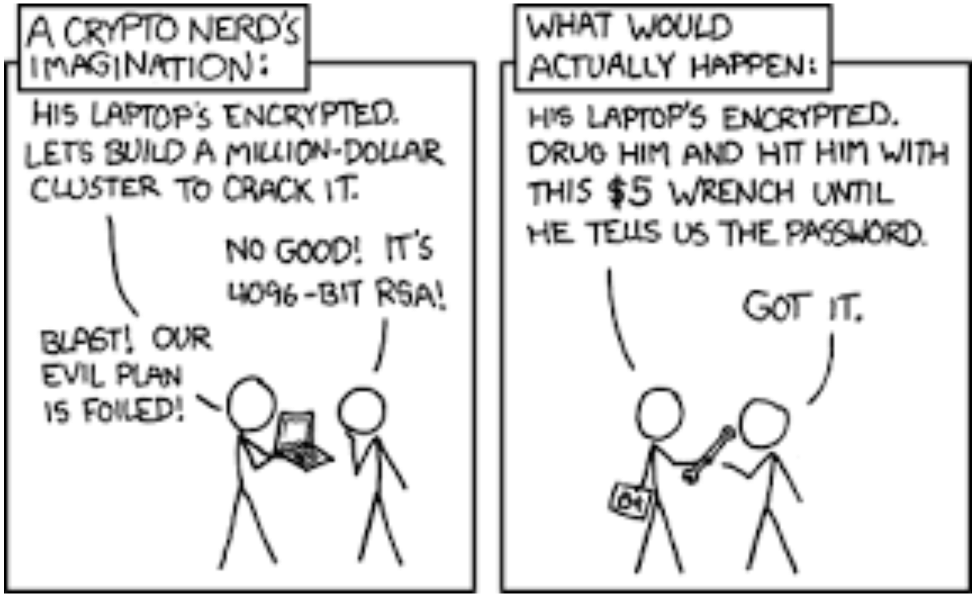
(a CXO and/or Board Member read a scary news report)

Compliance

(where I think the pendulum is swinging)

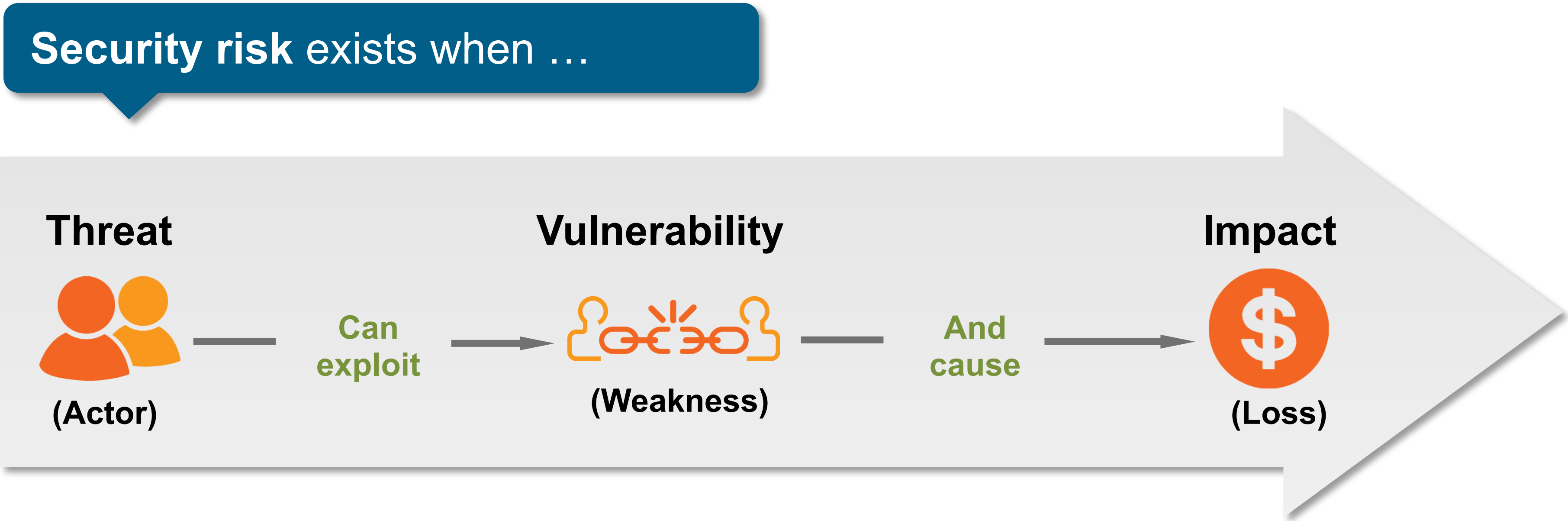
The Pragmatic Approach to Security Risk Management

- As a “theory” started gaining momentum in the late 1990s.
- Focuses on finding a balance between effective security and cost
- Belied by a fairly simple “Risk Equation”
- Most regulations/security best practice guides recognize this.


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LETS BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

The Axiom… Never spend $100 dollars on a fence to protect a $10 horse

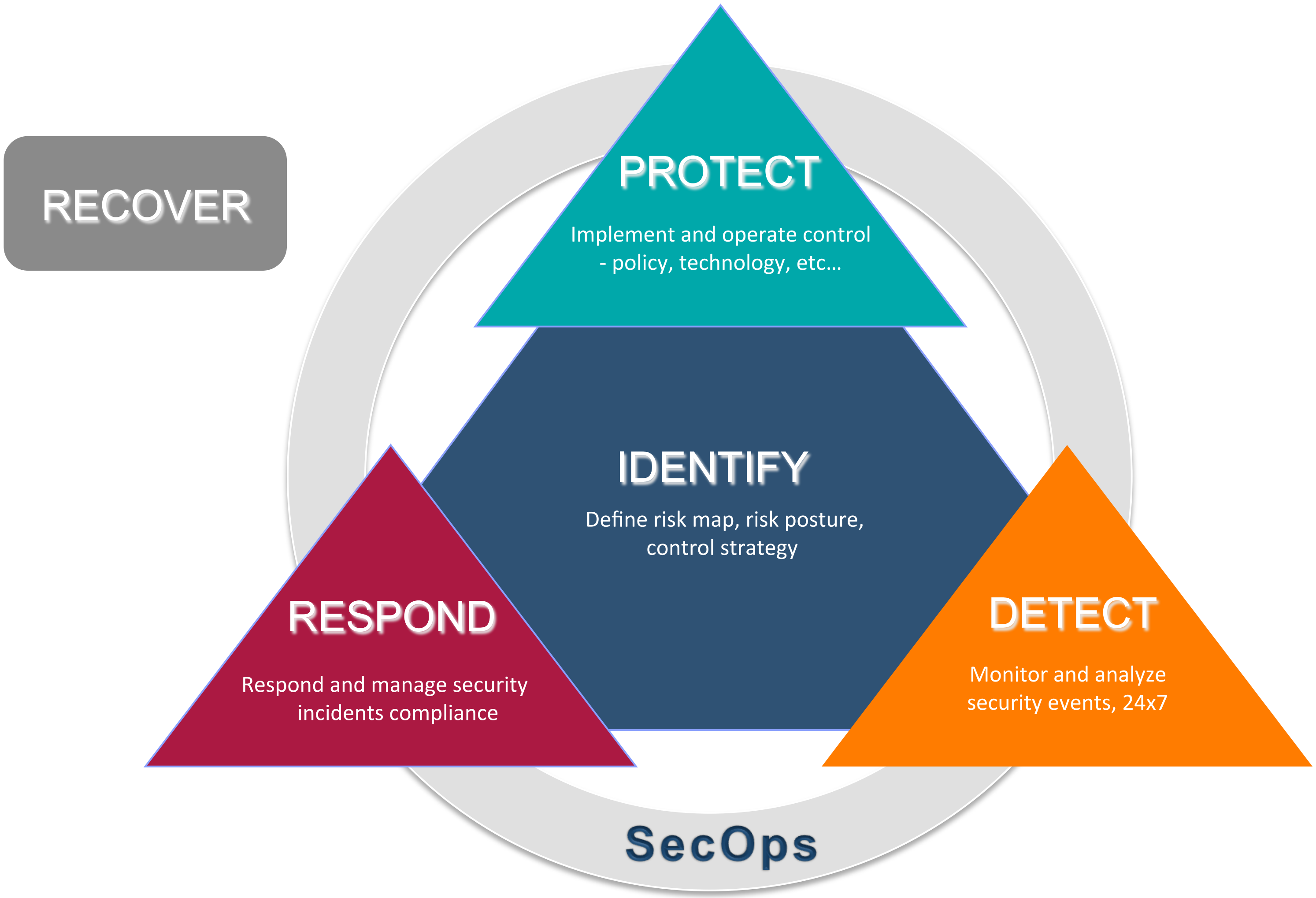
Thinking like a security expert



Security Risk Management is the application of **control…**

- to detect and block the **threat,**
- to detect and fix a **vulnerability,**
- or to address the **impact** when all else fails.

How pragmatic security risk management works



RECOVER

PROTECT

Implement and operate control - policy, technology, etc…

IDENTIFY

Define risk map, risk posture, control strategy

RESPOND

Respond and manage security incidents compliance

DETECT

Monitor and analyze security events, 24x7

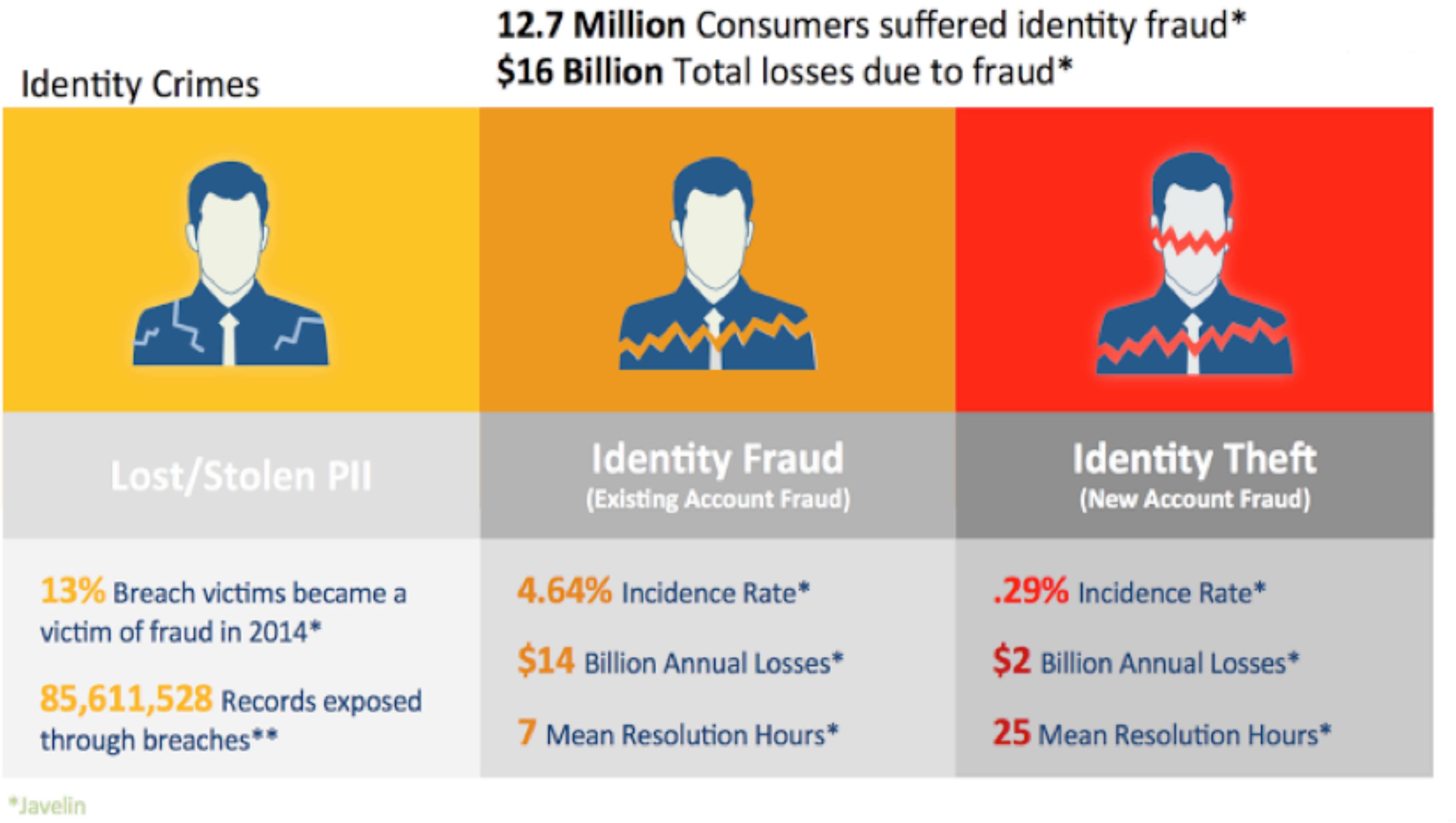
SecOps

BEWARE: Security Risk Management in REAL LIFE

Phase	People	Data	Apps	Endpoint	Server	Network
1. Identify	Policies, Education & Awareness, Role Managment	Policies, Data Classification (Manual)	Asset Management (CMDB)	Mobile Device Management/ Asset Management	Asset Management CMDB)	Asset Management CMDB)
2. Protect	Identity & Access Mgmt, **Biometrics**	**Encryption,** Digital Rights Mgmt	Web App FW, **Web & Email Filtering,** Access Control, Maintenance	AV, ADS, PFW, IPS, Configuration Mgmt. and Enforcement (MDM on Mobile), Maintenance	AV, IPS, Configuration Mgmt. and Enforcement, Access Control, Maintenance	FW, IDS/IPS Configuration Mgmt. and Enforcement, Access Control, Maintenance
3. Detect	Privileged use monitoring	DB Monitoring, Data Loss Prevention	Security Info & Event Mgmt,; AM & Fraud Detection	AV, Malware Gateway	Security Info & Event Mgmt,	IDS, Security Info & Event Mgmt, Malware Gateway
4. Respond	Varies	Data Privacy Team	Fraud/AML Team	Emergency Response Team	Emergency Response Team	Emergency Response Team
5 Recover						

*Areas of CONFLICT

Cyber Crime impact to the individual?



Identity Crimes

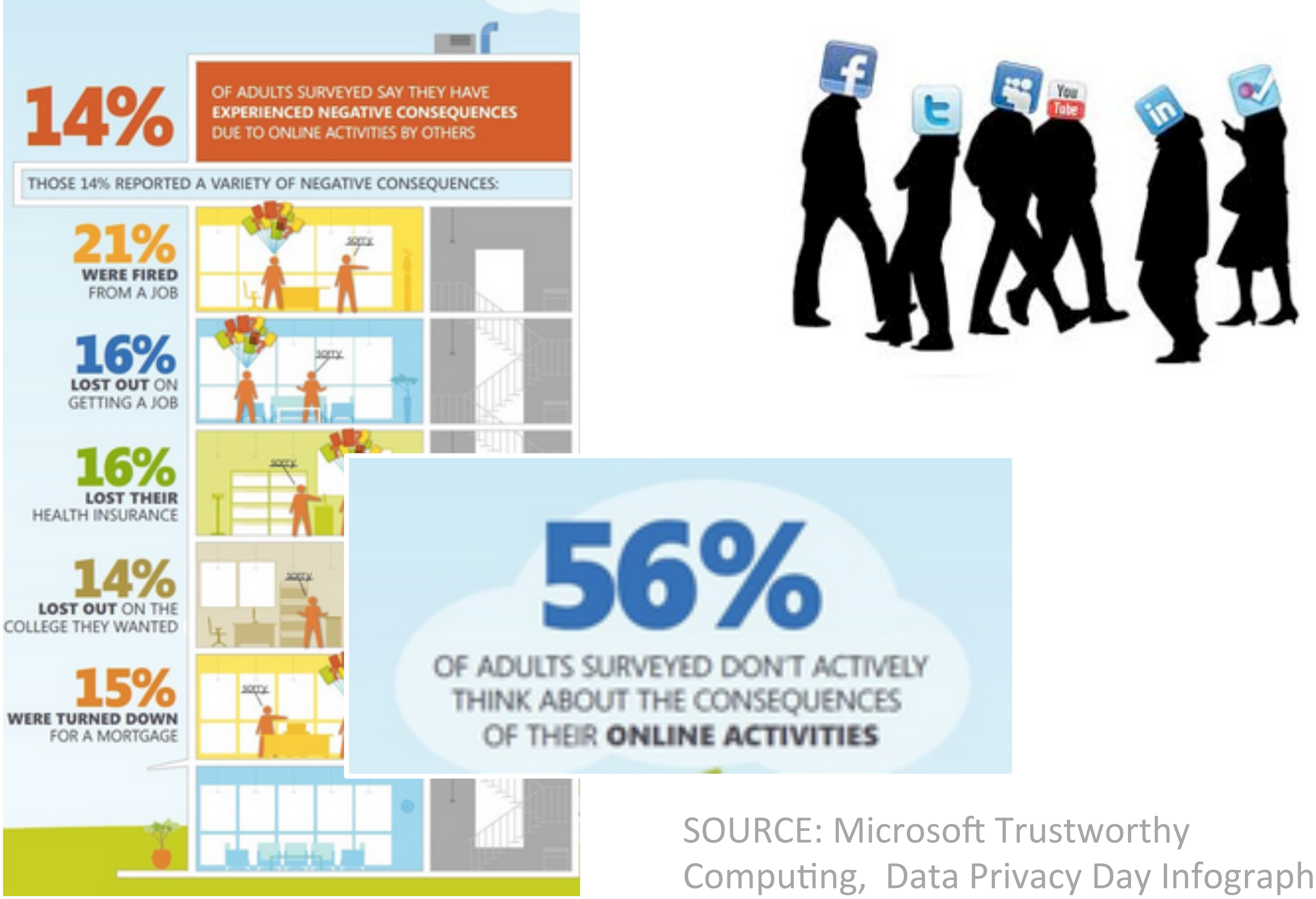
12.7 Million Consumers suffered identity fraud*
$16 Billion Total losses due to fraud*

Lost/Stolen PII	Identity Fraud (Existing Account Fraud)	Identity Theft (New Account Fraud)
13% Breach victims became a victim of fraud in 2014*	4.64% Incidence Rate*	.29% Incidence Rate*
85,611,528 Records exposed through breaches**	$14 Billion Annual Losses*	$2 Billion Annual Losses*
	7 Mean Resolution Hours*	25 Mean Resolution Hours*

*Javelin

Source: Javelin Identity Theft Statistics, 2015

Consumers don't always express concerns in practical terms


14%
OF ADULTS SURVEYED SAY THEY HAVE EXPERIENCED NEGATIVE CONSEQUENCES DUE TO ONLINE ACTIVITIES BY OTHERS
THOSE 14% REPORTED A VARIETY OF NEGATIVE CONSEQUENCES:
21% WERE FIRED FROM A JOB
16% LOST OUT ON GETTING A JOB
16% LOST THEIR HEALTH INSURANCE
14% LOST OUT ON THE COLLEGE THEY WANTED
15% WERE TURNED DOWN FOR A MORTGAGE
sorry
56%
OF ADULTS SURVEYED DON'T ACTIVELY THINK ABOUT THE CONSEQUENCES OF THEIR ONLINE ACTIVITIES
You Tube

SOURCE: Microsoft Trustworthy Computing, Data Privacy Day Infograph